P3P Implementation at FSA

Background

The E-Government Act requires that government agencies post their website security policies in machine readable language. Currently, the *de facto* standard for doing this is through P3P. This document serves as a high level overview of how FSA will implement P3P.

Preliminary Activities

FSA has already done a number of activities to start this initiative. The FSA Security and Privacy Team have done research on P3P to familiarize the Team and FSA with the basic concepts. FSA has communicated this information through its Online Security Center, http://fsanet.ed.gov/cio/products/it_security_portal/p3p/index.html, and through training for the system security officers.

Now that FSA has raised awareness on P3P, FSA has begun creating the implementation steps for P3P. FSA is planning on doing an enterprise wide implementation of P3P. Rather than having each system create its own P3P policies, which would likely result in contract modifications, the FSA CIO will work with the individual systems in the process. Working with the systems, the FSA CIO will determine which systems P3P applies to and with whom the FSA CIO should work to work. FSA CIO will create a uniform set of P3P policies; the individual systems will select the appropriate ones and put them on their web servers. Within FSA, there are common types of privacy policies; this will enable FSA CIO to create a standard set of policies.

Implementation Steps

FSA CIO will work with the system security officers to obtain preliminary privacy policy information. FSA CIO needs to determine which systems have websites that are publicly accessible. FSA Security will review the websites, in coordination with the security officers, to determine the different types of P3P policies the site will need and what privacy policies they have currently. FSA will document the content of existing policies. FSA also needs to know on which web server the websites are located. FSA Security will compile this information in an inventory for tracking purposes and will also use this information in the future for the P3P policy writing.

FSA will take the preliminary information and existing privacy policies and create the P3P policies for the enterprise. FSA may use the IBM P3P policy generator to create the policies.

After the policies are written, FSA will work with the systems and their contractors to have the P3P policies uploaded to their web servers. P3P policies need to be placed in a well-known location and FSA will work with the contractors to explain how this is typically done.

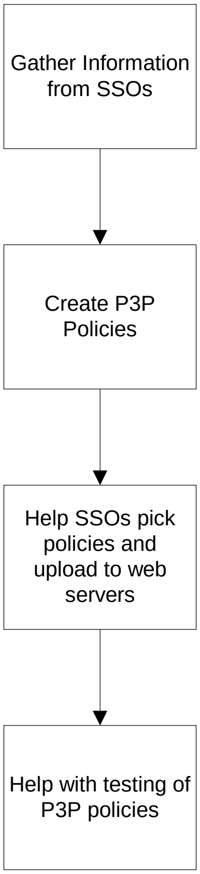
After the P3P policies have been uploaded and the reference files have been established, FSA Security will work with the contractors as needed for testing of the P3P policies. There is a P3P validator tool that will probably be used and several pages will be tested.

Once the policies have been uploaded and have passed the testing they will be ready to go live.

Reporting

FSA will keep the Department informed of their progress and will notify the Department when all of the P3P policies are implemented.

Diagram of Implementation Steps for FSA CIO


Gather Information from SSOs
Create P3P Policies
Help SSOs pick policies and upload to web servers
Help with testing of P3P policies